1. DRAFT HHS DEPARTMENT-WIDE STANDARDS

This document is subject to review and approval of the HHS CIO council.

1.1 Standards and Products

A detailed list of all HHS-approved standards and preferred COTS products is provided in Exhibit 1-2 below. Standards are grouped first by service area, then by specific classes of technology within each service area. The list serves to help define the HHS infrastructure, which supports the HHS Target Architecture.

The standards and products within each service area are discussed in greater detail in Sections 1.13 and 1.14. For each standard, the status, description, rationale, and implications for HHS are presented. Finally, Appendix 1-A provides a suggested list of candidate standards for future consideration.

It is important to note the distinction between the candidate standards which appear in Exhibit 1-2 and Section 1.13, and the suggested candidates which appear in Appendix 1-A. The former are standards which have been discussed and agreed on as candidates by the ITAG, while the latter are a selection of standards from external sources, which the ITAG will review for applicability at a later date.

Exhibit 1-2–HHS Technical Standards and Preferred Products Matrix

The Status column identifies the status of the system standard as follows:

- **A–** Recommended for adoption throughout the Department
- **C–** Candidate standard that requires more investigation prior to being recommended for adoption

The Class column identifies the classification of standard type as follows:

- **DF–**De facto standard
- **DJ–**De jure standard

Services	System Standards	Status	Class	Preferred Products
User Services				
Web-Based Interface	HTML(IETF RFC 1866)	A	DJ	Microsoft Internet Explorer Netscape Navigator
	XML (W3C Recommendation. XML 1.0)	A	DJ	
	JAVA Script (Netscape)	A	DF	
	DHTML	C	DF	
Application Services				
Directory Access	LDAP (IETF RFC 2251)	A	DJ	

Services	System Standards	Status	Class	Preferred Products
Email Access	IMAP v4.1(IEFT RFC 2060)	A	DJ	Microsoft Exchange
	SMTP (IETF RFC 821)	A	DJ	
	MIME (IETF RFC 2045, 2046, 2047, 2048, 2049)	A	DJ	
	S/MIME (IETF RFC 2632, 2633, 2634)	A	DJ	
Vector Graphics	CGM v3 (ISO 8632)	C	DJ	
Raster Graphics	JPEG (ISO 10918)	A	DJ	
	GIF (GIF89a)	A	DF	
Video Graphics	MPEG (ISO 11172, 13818)	A	DJ	
Programming Services				
Business Modeling	OMG UML v1.3	C	DJ	
Project Management	SEI CMM v1.1	C	DF	Microsoft Project
	ISO 9000-3	C	DJ	
Programming	Java 2, v 1.3 (Sun Microsystems, Inc.)	C	DF	
	ActiveX (Microsoft)	C	DF	
Date Management Services				
Data Base Management	SQL 92 (ISO 9075)	A	DJ	DB2, Oracle, SQL Server
	ODBC (Microsoft)	A	DF	
	JDBC (Sun Microsystems, Inc.)	C	DF	
Data Interchange Services				
Format	PDF (Adobe)	A	DF	Adobe Acrobat
Data Element Standardization	ISO 11179	C	DJ	
Object Brokers	CORBA 2.2 (OMG CORBA v 2.2)	A	DJ	
Office Automation	COM (Microsoft)	C	DF	Microsoft PowerPoint Microsoft Access Microsoft Excel Microsoft Word WordPerfect (Case Specific)
Network Services				
Cabling	100 MB + (IEEE 802.3u, 802.12)	A	DJ	
Transport	TCP/IP (IETF STD5/STD7)	A	DJ	
Directory Access	ANSI X.500	A	DJ	
	LDAP (IETF RFC 2251)	A	DJ	
Domain Naming	DNS (IETF STD13)	A	DJ	
Remote Access	PPP (IETF STD051)	A	DJ	
	VPN (IETF RFC 2401/2709)	A	DJ	

Services	System Standards	Status	Class	Preferred Products
Access	Carrier Sense Multiple Access/ Collision Detection (IEEE 802.3)	C	DJ	
Operating System Services				
Desktop				Windows 95/98/NT
Server	POSIX (ISO 9945)	C	DJ	
	X-Windows, X11R6 (Open Group C507, 508, 509, 510)	C	DJ	
Security Services				
Public Key Certificates	ANSI X.509	A	DJ	
	PKI	A	DJ	
	SSL	A	DF	
	IPSec (IETF RFC 2401)	A	DJ	
System Management Services				
Messaging	SNMP (IETF RFC 1441)	A	DJ	

1.2 Technical Standards

The following standards have been listed below by service area.

1.2.1 User Services

User interfaces are the most visible to the user. Within the past few years, significant advances have been made in interface technology in ease-of-use and reducing the development effort required. Depending on the capabilities required by users and the applications, these services may include dialogue support, window management, and multimedia specifications.

HTML Hypertext Markup Language (IETF RFC 1866)

Status: Recommend adoption

Description: The language used to create Web documents and is a subset of Standardized General Markup Language (SGML). Although most browsers display any document written in plain text, there are advantages to writing documents using HTML. When HTML documents are read by applications specifically designed for the Web, they can include formatting, graphics, and links to other documents.

Rationale: This is the de facto standard for Web browsers.

Implications:

- Cost Effective: Backward compatibility must be considered to ensure cost effectiveness
- Allows documents to be easily published and accessed via the Web. Provides the electronic publishing markup for the Web, but does not preserve page fidelity.

XML Extensible Markup Language (W3C Recommendation. XML 1.0)

Status: Recommend adoption

Description: Currently a formal recommendation from the WWW Consortium (W3C), XML is similar to HTML. Both XML and HTML contain markup symbols to describe the contents of a page or file. HTML, however, describes the content of a Web page (mainly text and graphic images) only in terms of how it is to be displayed and interacted with. XML extends this such that the attributes of the data can be defined and transferred by Web applications. This means that an XML file can be processed purely as data by a program or it can be stored with similar data on another computer or, like an HTML file, it can be displayed.

Rationale: This is the emergent standard for Web browsers.

Implications:

- XML files can be processed purely as data by a program or can be stored with similar data on another computer or, like HTML files, they can be displayed

HTML/Java Script (Netscape)

Status: Recommend adoption

Description: JavaScript is a programming environment used to create dynamic HTML pages that process user input and maintain persistent data using special objects, files, and relational databases.

Rationale: The core language corresponds to ECMA-262, the scripting language standardized by the European standards body.

Implications:

- JavaScript has become an industry-accepted standard, supported by all major browsers. It will be come a major programming tool set as the number of Web-enabled applications grows.

DHTML Dynamic HTML

Status: Candidate

Description: Dynamic HTML is a collective term for a combination of new HTML tags and options, style sheets, and programming that will allow Web pages that are more animated and more responsive to user interaction than previous versions of HTML. Much of dynamic HTML is specified in HTML 4.0.

Rationale: There is no single specification for "dynamic HTML"; it is a combination of several programming tools. Netscape and Microsoft each have their own definitions and explanations of it on their respective Web sites As style capabilities are accepted, and expected, by users, the different implementations will begin to merge into a true standard.

Implications:

- Style Sheets must be tested for results in different browsers
- Programmers using DHTML must develop separate pages to support the different available browsers.

1.2.2 Application Services

Application services are often the most complex part of system development and maintenance. Within the past few years, significant advances have been made in application technology in ease-of-use and reducing the development effort required. Depending on the capabilities required by users and the applications, these services may include the following: client/server operations, object definition and management, dialogue support, window management, and multimedia specifications.

1.2.2.1 Directory Access

LDAP Light Directory Access Protocol (IETF RFC 2251)

Status: Recommend adoption

Description: The protocol is designed to provide access to directories supporting the X.500 models, while not incurring the resource requirements of the X.500 Directory Access Protocol (DAP).

Rationale: LDAP is a vendor-independent, open, network protocol standard. It is platform-independent and supports multi-vendor interoperability in the same fashion as TCP/IP, Simple Mail Transport Protocol (SMTP), Domain Name Space (DNS), and others. The LDAP protocol also directly supports various forms of security (authentication, privacy, and integrity) technology, runs directly over TCP, and provides critical X.500 functionality at a much lower cost.

Implications:

- LDAP implementation allows for remote directory access and standardization.

1.2.2.2 E-mail Access

IMAP, v.4.1 Internet Message Access Protocol (IEFT RFC 2060)

Status: Recommend adoption

Description: The Internet Message Access Protocol, Version 4rev1 (IMAP4rev1) allows a client to access and manipulate electronic mail messages on a server. IMAP4rev1 permits manipulation of remote message folders, called "mailboxes", in a way that is functionally equivalent to local mailboxes. IMAP4rev1 also provides the capability for an offline client to resynchronize with the server

Rationale: IMAP allows remote client/server capabilities between the client and mail server, and provides greater capability than POP3. The major Email server vendors support IMAP.

Implications:

- Allows remote access to email.
- Server storage space requirements will be higher.

SMTP Simple Mail Transfer Protocol (IETF RFC 821)

Status: Recommend adoption

Description: This is a TCP/IP protocol that facilitates transfer of E-mail messages. It specifies how two systems are to interact, and the messages format used to control the transfer of E-mail.

Extensible Simple Mail Transfer Protocol (ESMTP) is by definition extensible, allowing new service extensions to be defined and registered with IANA

Rationale: All HHS OpDivs/Offices employ SMTP, which is supported by almost all communications products suppliers.

Supports Internet E-mail. Users can send E-mail from any computer, but must have an account (post office box) on a host system in order to receive mail from others. Many non-Internet commercial services and government agencies have SMTP “gateways” that allow users to send and receive E-mail over the Internet.

Implications: None.

MIME Multipurpose Internet Mail Extensions (IETF RFC 2045, 2046, 2047, 2048, 2049)

Status: Recommend adoption

Description: This extension to Internet E-mail allows transmission of non-textual data, such as graphics, audio, video, and applications data (e.g., spreadsheets and word processing documents). MIME was designed to overcome the inability of SMTP to handle binary data. Message parts can also be labeled to identify to the recipient or to the mail software the type of data contained within the attachment to determine how it should be handled. It is the core Internet standard for multimedia E-mail and a building block of Hypertext Transport Protocol (HTTP)

When an E-mail message with a file attachment (e.g., Word document) is sent across the internet MIME converts the binary attachment to a text format that can be handled by internet E-mail. The recipient needs a program that decodes the MIME E-mail and turns it back into a binary file that can be read by the relevant application (e.g., Microsoft Word)

Rationale: MIME is a proven standard with many implementations.

MIME Supports multimedia Internet E-mail and HTTP. MIME is supported by almost every communications products supplier.

Implications:

- Facilitates delivery
- Does not guarantee usability
- Does not assume that the necessary application will be on the desktop

S/MIME Secure Multi-Purpose Internet Mail Extensions (IETF RFC 2632, 2633, 2634)

Status: Recommend adoption

Description: S/MIME is a secure method of sending e-mail that uses the Rivesd, Shamir, and Adleman (RSA) encryption system. It provides specifications for E-mail security exploiting cryptographic message syntax in an internet MIME environment

Rationale: Enables providers to protect important and sensitive information sent internally and externally to HHS.

Enables the encryption and authentication of messages and attachments using digital certificates

Certifies who has created and signed messages

Implications:

- Prevents users or invalid parties from intercepting, capturing, viewing or modifying sensitive HHS information
- Can prevent external message creators from masking their true identity or posing as HHS users

1.2.2.3 Vector Graphics

CGM Computer Graphics Metafile (ISO 8632)

Status: Candidate

Description: CGM provides definitions for structure and transfer of vector graphics data.

Rationale: CGM is the best supported vector graphics format.

Implications:

- Supports cross-platform standard for vector graphics
- Use is indicated for publishing applications

1.2.2.4 Raster Graphics

JPEG Joint Photographic Experts Group (ISO 10918)

Status: Recommend adoption

Description: JPEG provides multiple levels of compression for raster graphics, reducing the size of the image.

Rationale: JPEG is supported by almost all desktop and client/server image manipulation applications.

Implications:

- Allows cross-platform transfer of graphic images.
- Supports consistency in graphics between applications.

GIF Graphical Interchange Format (GIF89a)

Status: Recommend Adoption

Description: GIF uses the 2D raster data type, is encoded in binary, and uses Abraham Lempel, Jacob Ziv, and Terry Welch (LZW) compression. There are two versions of the format, 87a and 89a. Version 89a (July, 1989) allows for the possibility of an animated GIF, which is a short sequence of images within a single GIF file.

Rationale: On the Web and elsewhere on the Internet (for example, bulletin board services), the GIF has become a de facto standard form of image.

Implications:

- The LZW compression algorithm used in the GIF format is owned by Unisys

MPEG Moving Pictures Expert Group (ISO 11172, 13818)

Status: Recommend adoption

Description: The Moving Picture Experts Group develops standards for digital video and digital audio compression under the auspices of the International Organization for Standardization (ISO). The MPEG standards are an evolving series, each designed for a different purpose.

Rationale: MPEG standards are used throughout the internet community to transfer streaming audio and video. ISO sponsorship provides for compatibility over time.

Implications:

- The MPEG standards are an evolving series.
- Files tend to be large.

1.2.3 Programming Services

The objectives of open systems are production and use of portable, scalable, interoperable software. Programming services provide the infrastructure to develop and maintain software that exhibits the required characteristics. Standard programming languages and software engineering methodologies, tools, and environments become central to this objective. While applications do not necessarily make direct use of programming services, without these services process automation would be more difficult and error-prone.

1.2.3.1 Business Modeling

UML v1.3 Unified Modeling Language (OMG UML 1.3)

Status: Candidate

Description: The UML standard has been developed to support specifying, constructing, visualizing, and documenting the artifacts of a software-intensive system.

Rationale: Utilizing CASE tools which support the UML will allow software engineering work to be shared between projects, even if the tools are different.

Implications:

- Currently there is very limited use of modeling within the Department.
- As the language specification evolves, and more tools support it, the standard will become more relevant.

1.2.3.2 Project Management

SEI CMM v.1.1 Capability Maturity Model (SEI CMM v1.1)

Status: Candidate

Description: The CMM describes the essential elements of an organization's systems engineering process that must exist to ensure good systems engineering.

Rationale: Utilizing the essential elements will help make the software engineering process more efficient and effective.

Implications:

- Department policy on software engineering is under review, and CMM is being considered as part of that review.

ISO 9000-3 Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software

Status: Candidate

Description: Guidance for the development, supply, installation, maintenance and supply of computer software.

Rationale: Provides the user with specific interpretation of the quality ISO-9001 standards for computer software.

Implications:

- Department policy on software engineering is under review, and ISO 9000-3 is being considered as part of that review.

1.2.3.3 Programming

Java Java 2, v 1.3 (Sun Microsystems, Inc.)

Status: Candidate

Description: Java is a programming language, owned by Sun Systems, expressly designed for use in the distributed environment of the Internet. It was designed to have the "look and feel" of the C++ language, but it is simpler to use than C++ and enforces a completely object-oriented view of programming. Java can be used to create complete applications that may run on a single computer or be distributed among servers and clients in a network.

Rationale: Programs are portable in a network; Java is object-oriented, executed at the client rather than the server; Java is easier to learn relative to C++.

Implications:

- Supports object-oriented programming.
- Java virtual machines available for most major platforms.

Active X (Microsoft)

Status: Candidate

Description: ActiveX is the name Microsoft has given to a set of "strategic" object-oriented program technologies and tools. A self-sufficient program that can be run anywhere in an ActiveX network is known as an ActiveX control.

Rationale: An ActiveX control can be created using one of several languages or development tools, including C++ and Visual Basic, or PowerBuilder, or with scripting tools such as VBScript.

Implications:

- Strategic competitor with Java classes.
- Component of Microsoft’s COM/DCOM architecture.

1.2.4 Data Management Services

Data Management Services provide for the independent management of data shared by multiple applications. These services support definition, storage, and retrieval of data elements. Data management services provide the functions to establish data dictionary and directory services, database management systems, and access to distributed data.

SQL 92 Structured Query Language (ISO 9075)

Status: Recommend adoption

Description: SQL-92 is the current standard for relational database management systems (RDBMS), defining the syntax for the creation, manipulation and deletion of data within a relational model.

Rationale: Due to the time SQL-92 has been available, almost all RDBMSs can send and receive data in the SQL-92 format, and support the SQL-92 language syntax.

Implications:

- SQL 92 supports multi-tiered applications
- Allows remote calls between different platforms
- Will not fully support object-oriented databases as they evolve.

ODBC Open Database Connectivity (Microsoft)

Status: Recommend adoption

Description: ODBC is Microsoft's implementation of the Call Level Interface described in ISO 9075-3. It provides a vendor-provided driver for applications to access data from the RDBMS.

Rationale: Provides desktop application access to multi-tier RDBMS engines with reduced API coding. Although only a subset of the Command Line Interface (CLI) standard, it has been supported by most RDBMS vendors.

Implications:

- Desktop oriented

JDBC Java Data Base Connectivity (Sun Microsystems)

Status: Candidate

Description: Java Database Connectivity, a Java Application Programming Interface (API) that enables Java programs to execute SQL statements. This allows Java programs to interact with any SQL-compliant database.

Rationale: Because Java itself runs on most platforms, JDBC makes it possible to write a single database application that can run on different platforms and interact with different DBMSs.

Implications:

- Used with Java applications

1.2.5 Data Interchange Services

Data Interchange Services provide specialized support for the exchange of information, including format and semantics of data entities between applications on the same or diverse platforms.

PDF Portable Document Format (Adobe)

Status: Recommend adoption

Description: PDF is associated with the Adobe Acrobat product suite. PDF provides for the final form delivery of information in a standardized platform-independent electronic format. A proposed specification is being developed that retains the page layout and pictorial information needed for complex document delivery. The portable, final form document is created from the revisable form document using conversion applications.

Rationale: Allows documents to be displayed in a manner that is independent of the original application software, hardware, or operating system used to create them. The file can describe documents containing text, graphics, and images that can be viewed and printed from Windows, Macintosh, or UNIX systems.

Implications:

- Allows for costs savings in the following areas: Preserves page fidelity; supports multi-platform; free viewers for users; unnecessary software conversion and use; ease-of-use in an electronic medium; storage and paper cost savings; and a new way to preserve documents.

ISO 11179 Specification and standardization of Data Elements

Status: Candidate

Description: ISO/IEC 11179 is a set of six standards that promote the sharing and reusability of data throughout an organization and between the organization and other external organizations by providing guidelines for attribute specification standardization.

Rationale: ISO 11179 provides for standardized descriptions and structure of like data, improving portability and reuse. It also reduces the duplication of data.

Implications:

- Policy oriented.
- To be considered in future policy reviews.

CORBA 2.2 Common Object Request Broker Architecture (OMG CORBA v 2.2)

Status: Recommend adoption

Description: The CORBA standard describes the mechanism for brokers from different vendors to pass valid information back and forth.

Rationale: CORBA allows objects to be correctly identified and manipulated across multiple systems and multiple vendors.

Implications:

- Distributed Component Object Model (DCOM) does not support CORBA, though a gateway agreement is reported.
- Some vendors are still supporting Distributed Computing Environment (DCE), requiring a bridge between the two architectures.

COM Component Object Model (Microsoft)

Status: Candidate

Description: The Microsoft Component Object Model (COM) is a software architecture that allows applications to be built from binary software components.

Rationale: COM is the basis for many Microsoft applications and APIs. If a WINTEL desktop is the Departmental standard, the model fits with the desktop operating environment.

Implications:

- Microsoft proprietary.

1.2.6 Network Services

Network Services provide connectivity and basic services to foster communications across workgroups and sites. These services comprise the network infrastructure to provide the capabilities and mechanisms to support distributed data access and interoperability in a heterogeneous environment. Components of this category include data communications, E-mail services, directory services, transparent file access/transfer, remote network access, and remote procedure call.

1.2.6.1 Cabling

100 MB + Cable Connection (IEEE 802.3u, 802.12)

Status: Recommend adoption

Description: Institute of Electrical and Electronics Engineers (IEEE) provides detailed specifications for the composition, implementation and testing of data cable connections. With the existing and projected bandwidth requirements increasing for both backbone and workstation connections, a minimum of 100 Mega Bytes capacity is required for new installations and rewiring projects.

Rationale: Both copper and fiber cable are in use for backbone and workstation installations. By allowing for any standard supporting 100 MB and above, future installations will be able to support the current industry standard.

Implications:

- Installation testing is the key to meeting bandwidth requirements.
- Both copper and fiber are supported.

1.2.6.2 Transport

TCP/IP TCP/IP and its suite of protocols (IETF STD5,STD7)

Status: Recommend adoption

Description: TCP/IP is a well established, widely adopted industry standard communications protocol. It is the primary means of communications throughout the Internet. TCP/IP provides for a reliable, connection-oriented, end-to-end transport service on top of an unreliable network that can lose, garble, store, and duplicate packets. TCP resembles the OSI Transport Protocol class 4 (TP4), but major differences exist in features, such as handling collisions, addressing format, quality of service, use of user data during set-up of a connection, handling "important data," absence of piggybacking in TP4, kind of message streams, flow control handling, window numbering scheme, and connection release. Associated with TCP is a network layer protocol called Internet Protocol or IP. The IP address structure is inefficiently used at present, which will ultimately result in exhausting Internet addresses. In order to resolve the address limitation problem, IP Version 4 is being revised. The new generation IP (IP Version 6 - also known as Ipng) will alleviate the address depletion problems.

Rationale: Adopting TCP/IP network protocol will simplify communications and data exchange among Internet connected devices and entities. TCP/IP is the only widespread non-proprietary transport protocol standard. TCP/IP supports File Transfer Protocol, Simple Mail Transfer Protocol, and TELNET (remote login). TCP/IP is supported by almost every supplier of communications products.

Implication:

- TCP/IP can be used over almost any kind of network to provide quality end-to-end transmission service.

X.500

Status: Recommend adoption

Description: A Committee on International Telephone and Telegraphy (CCITT) protocol, X.500 is a family of standards and uses a distributed approach to realize a global directory service. Local (communication-oriented) information of an organization is maintained locally in one or more so-called directory system agendas (DSAs). "Local" is a flexible expression and it is possible that one DSA keeps information for more than one organization. The opposite is also possible; directory data of one large organization can reside in multiple DSAs, which are still considered local from a service-provision point of view.

Rationale: X.500 offers the following features: decentralized maintenance; powerful searching capabilities; single global name space; and structured information framework that allows local extensions.

Implication:

- Provides directory services interoperability among heterogeneous computer systems.

LDAP Lightweight Directory Access Protocol (IETF RFC 2251)

Status: Recommend adoption

Description: LDAP is a protocol for accessing online directory services. It runs directly over TCP, and can be used to access a standalone LDAP directory service or a directory service that is back-ended by X.500. The LDAP standard defines: a network protocol for accessing information in the directory; an information model defining the form and character of the information; a name space defining how information is referenced and organized; and an emerging distributed operation model defining how data may be distributed and referenced (v3). Both the protocol itself and the information model are extensible. Details of LDAP are defined in RFC 1777, "The Lightweight Directory Access Protocol."

Rationale: LDAP is a vendor-independent, open, network protocol standard. It is platform-independent and supports multi-vendor interoperability in the same fashion as TCP/IP, SMTP, DNS, and others. The LDAP protocol also directly supports various forms of strong security (authentication, privacy, and integrity) technology.

Runs directly over TCP and provides most of the functionality of full X.500 at a much lower cost.

Implications:

- A common schema needs to be established within HHS to provide LDAP gateway.

DNS Internet Domain Name System (IETF STD13)

Status: Recommend adoption

Description: DNS introduces domain style names, their use for Internet mail and host address support, and the protocols and servers used to implement domain name facilities. This online distributed database translates human readable domain names into numeric IP addresses and vice versa.

This provides the Internet addressing scheme.

Rationale: Identifies Internet locations for interchange.

Implications:

- Difficult to implement DNS across the Department

PPP Point-to-Point Protocol (IETF STD051)

Status: Recommend adoption

Description: The PPP provides asynchronous connectivity over telephone lines to network gateways, allowing modem connectivity to a network.

Rationale: PPP is used by most service providers, and supported by all desktop operating systems. SLIP, the major alternative, does not provide the throughput of PPP.

Implications:

- Allows for remote dial-up access.
- Used by Internet Service Providers.
- Integrates with Virtual Private Networks.

VPN Virtual Private Network protocol (IETF RFC 2401, 2709)

Status: Recommend adoption

Description: Virtual Private networks are evolving to provide the security needed to transport data across public lines.

Rationale: As the standards evolve, VPN will become a secure transport mechanism for corporate and other sensitive data, and support data integrity by authentication of source and destination.

Implications:

- Lower level protocols are still evolving.
- RFC compliance will not yet guarantee multi-vendor compatibility.

1.2.6.3 Access:

CSMA/CD Carrier Sense Multiple Access/Collision Detection (IEEE 802.3)

Status: Candidate

Description: Carrier Sense Multiple Access/ Collision Detection, popularly called Ethernet, allows packets to be broadcast by any station, and includes logic to reschedule transmissions if a collision is detected.

Rationale: 802.3 provides reasonable throughput with relatively low overhead, and ease of installation.

Implications:

- Ethernet is the major Local Area Network access method. Ethernet has industry support in applications, components and training.

1.2.7 Operating System Services

Operating system services provide the software environment and base interfaces within all computing devices to function while maximizing machine resources and capabilities.

1.2.7.1 Desktop

Windows Windows 95/98/NT (Microsoft)

Status: Recommend adoption

Description: Windows, in its multiple versions, is the industry standard for general desktop computing, providing a Graphical User Interface (GUI), 32-bit processing, and a large suite of Application Programming Interfaces (APIs) for use by 3d party applications developers.

Rationale: Supports most Departmental Office automation standard products and many other COTS applications.

Implications:

- Version control can be an issue; service releases can impact application performance.

1.2.7.2 Server

POSIX (ISO 9945)

Status: Candidate

Description: Portable Operating System Interface (POSIX)is a set of standard operating system interfaces based on the UNIX operating system.

Rationale: POSIX is intended to be one part of the suite of standards (a "profile") that a user might require of a complete open system.

Implications:

- POSIX compliance does not guarantee application portability

X Windows: X11R6 (Open Group C507, 508, 509, 510)

Status: Candidate

Description: The X Window System (sometimes referred to as "X" or as "XWindows") is an open, cross-platform, client-server system for managing a windowed graphical user interface in a distributed network.

Rationale: The specifications and source code are freely available. As a result, it has been widely accepted by the computer industry.

Implications:

- Additional applications are required to run from a Win95/95/NT workstation.
- Primarily a UNIX/POSIX interface.

1.2.8 Security Services

The HHS information architecture should follow an accepted set of security services in order to ensure the integrity of mission critical information.

X.509 v3 Certificates (ANSI X.509)

Status: Recommend adoption

Description: As part of the X.509 protocol, certificates are assigned by a trusted Certificate Authority (issuing authority) and provide verification of a party's identity and may supply its public key. The X.509 is the International Telecommunications Union-T (ITU-T) standard for certificates. X.509 v3 refers to certificates containing or capable of containing extensions.

Rationale: Ensures that information sent or received can be validated and authenticated. Verifies that the originator of a document is a trusted entity.

Provides the ability to grant or deny user access to information resources and systems.

Provides the ability to assign rights or privileges to individuals or systems.

Implications:

- A centralized mechanism for issuing certificates is necessary to economically and practically achieve the functional benefits enterprise-wide

PKI Public Key Infrastructure

Status: Recommend adoption

Description: A PKI enables users of a basically non-secure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. PKI provides for digital certificates that can identify individuals or organizations and directory services that can store and, when necessary, revoke them. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on key.

Rationale: Ensures privacy.

Implications:

- Ability to set up Virtual Private Networks
- Private key used for encrypted signatures must not be compromised

SSL/TLS Secure Socket Layer, v3 (Netscape)

Status: Recommend adoption

Description: SSL is a program layer created by Netscape for managing the security of message transmissions in a network. Netscape's idea is that the programming for keeping your messages confidential ought to be contained in a program layer between an application (such as a Web browser or HTTP) and the Internet's TCP/IP layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. Netscape's SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. SSL has been renamed as Transport Layer Security (TLS) by the Internet Engineering Task Force (IETF).

Rationale: SSL is an integral part of each Netscape browser. If a Web site is on a Netscape server, SSL can be enabled and specific Web pages can be identified as requiring SSL access. Other servers can be enabled by using Netscape's SSLRef program library which can be downloaded for noncommercial use or licensed for commercial use.

Implications:

- A centralized mechanism for issuing certificates is necessary to economically and practically achieve the functional benefits enterprise-wide

IPSEC Internet Protocol Security (IETF RFC 2401)

Status: Recommend adoption

Description: IPSec is a developing standard for security at the network or packet processing layer of network communication. Earlier security approaches have inserted security at the application layer of the communications model. IPSec will be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks.

IPSec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header. Separate key protocols can be selected, such as the ISAKMP/Oakley protocol.

Rationale: A big advantage of IPSec is that security arrangements can be handled without requiring changes to individual user computers.

Implications:

- This is an emergent standard.
- HHS will be strategically positioned with the latest market technology standard.

1.2.9 System Management Services

System management services provides the mechanisms to monitor and control the operation of individual applications, databases, systems, platforms, networks, and user interactions with these components at all levels.

SNMP, v2 Simple Network Management Protocol (IETF RFC 1441)

Status: Recommend adoption

Description: SNMP describes a network management system containing agents, which have access to management instrumentation; at least one management station; and a management protocol used to convey management information between the agents and management station(s).

Rationale: SNMP has been the standard protocol (IETF STD 15) since 1990 for transferring information between network components, and is supported by all major vendors.

Implications: None

1.2.10 Hardware Platform Services

Hardware Platform Services vary enormously between, and even within, OpDivs/Offices. Hardware needs are generally very specific to the application, user and capacity requirements for a system.   Hence, it has been decided that standards for this area will not be established at this point in time.

1.3 Products

This section contains a representative set of preferred products for each of the services described in the previous section. The ITAG elected to standardize on products where it was in the best interest of HHS (i.e. interoperability, economies of scale and reduced training on multiple products). Appendix 1-A contains the HHS Technical Standards and Target Products Matrix that relates standards to products.

The products listed here are preferred software products for HHS and contractor use. It should be noted that the preferred software products are not the standards, but are products that satisfy the standards and/or that are preferred for use within HHS.

1.3.1 User Services

User interfaces are the most visible to the user. This area defines the methods by which people can interact with an application

Product	Description
Microsoft Internet Explorer	Web Browser supporting HTML 4 and earlier
Netscape Navigator	Web Browser supporting HTML 4 and earlier

1.3.2 Application Services

Application services are often the most complex part of system development and maintenance. This area provides the functions required for creating and manipulating displayed images, multimedia, client/server operations, etc. This service can be characterized as workstation functions.

Product	Description
Microsoft Exchange	E-mail server. MS Outlook is the bundled client.

1.3.3 Programming Services

This service area provides the structure to develop and maintain software that exhibits desired characteristics. This includes languages, tools, and methodologies.

Product	Description
Business Modeling	None
Microsoft Project	Project Management Application
Programming	None

1.3.4 Data Management Services

Data Management Services are central to HHS information systems and include definition, management, query, and security of data and structures.

Product	Description
IBM DB2	Relational Database Management System; available for client, server, or mainframe
Oracle	Relational Database Management System; available for client, server, or mainframe
Microsoft SQL Server	Server-based relational database management system

1.3.5 Data Interchange Services

Data Interchange Services provide specialized support for representing, storing, accessing, and transmitting data (primarily through formats) between applications on the same or different formats

Product	Description
Microsoft Word	Word Processing application
Word Perfect***	Word Processing application
Microsoft Excel	Spreadsheet application
Microsoft PowerPoint	Presentation graphics application
Microsoft Access	Desktop database management system
Adobe Acrobat	Document preparation application

**** Use of this application is case specific (i.e. cases where it is better suited for interchanges with other government entities outside HHS, legal work, etc.)*

1.3.6 Operating Systems Services

Operating system services are the core services needed to operate and administer the application's platform. They also provide an interface between the application software and the platform.

Product	Description
Microsoft Windows 95 or better	Microsoft 32-bit Operating system for Intel-based desktop workstations.
Server	No preferred product selected Predominantly used products in HHS: • NT • Novell • Banyan (being phased out) MS 2000 is an emergent product being evaluated for future use

Appendix 1-A—Suggested List of Candidate Standards

APPENDIX 1-A—SUGGESTED LIST OF CANDIDATE STANDARDS

HHS Service Area		Candidate Standards
Operating System Services		
Mainframe		POSIX.1, POSIX.2
Decision Support System		POSIX.1, POSIX.2
Office Automation Server		Win32
Programming Services		
Programming Language: C		ANSI/ISO/IEC 9899:1992; FIPS 160C
Programming Language: COBOL		ISO 1989:1985; ANSI X3.23a-1989, X3.23b-1993; FIPS 21-4 COBOL
Analysis of COBOL Code		Tools to enforce standards for COBOL
Analysis of C Code		Tools to enforce standards for C
Requirements Traceability		Tools to Support ELC deliverables
Analysis		Tools to Support ELC deliverables
Design		Tools to Support ELC deliverables
Configuration Management		Tools to support CM process
CASE Data Interchange Format (CDIF)		Electronic Industries Association (EIA) IS-106 to IS-121
Function Modeling Language		FIPS 183 Integration Definition for Function Modeling (IDEF0)
Information Modeling Language		FIPS 184 Integration Definition for Information Modeling (IDEF1X)
Object Oriented (OO) Programming Language: C++		ANSI 14882-1998 C++ Language
Data Management Services		
Decision Support System		127-2 Database Language SQL, ISO/IEC
Data Interchange Services		
Document Interchange		ANSI/ISO 8879:1986; FIPS 152 Standard Generalized Markup Language (SGML)
Electronic Data Interchange		ISO 9735:1988 UN/EDIFACT; ANSI ASC X12 EDI; FIPS 161-1 Electronic Data Interchange
Network Services		

Application Layer	Network Management	Management Information Base (MIB-II) (RFC 1213);
		Concise MIB Definitions (RFC 1212);

		FIPS 179-1 Government Network Management Protocol (GNMP)

		Simple Network Management Protocol (SNMP) Version 2:
		Standard Network Management Framework Versions 1 and 2 Coexistence (RFC 1908);
		ISO 9595: OSI-Common Management Information Service (CMIS) Definition;
		ISO 9596: OSI-Common Management Information Protocol (CMIP) Specification

Network Layer	Network Services	IP: IPv6 Specification (RFC 1883) IP: IPv6 ICMPv6 (RFC 1885); IP: Transition Mechanisms for IPv6 Hosts & Routers (RFC 1933)

HHS Service Area		**Candidate Standards**

	IP over ATM Services	IAB IP:
		IP: Classical IP and ARP over ATM (RFC 1577);
		IP: IP MTU over ATM AAL5 (RFC 1626);
		IP: ATM Signaling for IP over ATM (RFC 1755);
		IP: Real-Time Services for IP over ATM (RFC 1821);
		IP: IP over ATM Framework (RFC 1932)

	WAN Services	ISO 3309: High-Level Data Link Control (HDLC) Specifications ISO 7776: HDLC-Link Access Procedure - Balanced (LAPB) Industry/Government Open Systems Specification (IGOSS), NIST Special Publication 500-217 NIST ISDN Application Software Interface (ASI) Version 1 FIPS 182 Integrated Services Digital Network (ISDN); ITU-T I.120 ISDN ANSI T1.5 ATM; TA 1111; TA 1113 IEEE 802.6/ISO 8802-6 Distributed Queue Dual Bus (DQDB)
Data Link Layer	LAN Services	ISO 9314: Fiber Distributed Data Interface (FDDI) IGOSS NIST Special Publication 500-217
Physical Layer	FDDI Services	ISO 9314-1 FDDI Physical Layer Protocol (PHY) ISO 9314-3 FDDI Physical Medium Dependent (PMD)
	Carrier Services	**ANSI T1.403 Digital Signal DS1;** **ANSI T1.404 DS3**
Security Services		
Mainframe Operating System (OS)		DOD 5200.28-STD (C2 Implementation)
Decision Support System		**Secure Sockets Layer (SSL)**
Office Automation Server		**Secure Sockets Layer (SSL)**
Internet/Intranet		**Secure Sockets Layer (SSL)**
Cryptographic Technology		FIPS 46-2 Data Encryption Standard (DES)
		FIPS 81 Data Encryption Standard (DES) Modes of Operation
		FIPS 113 Computer Data Authentication
		FIPS 140-1 Security Requirements for Cryptographic Modules
		FIPS 171 Key Management Using ANSI X9.17
		FIPS 180-1 Secure Hash Standard (SHS)
		FIPS 186 Digital Signature Standard
		FIPS 196 Public Key Cryptographic Entity Authentication Mechanisms
		ANSI X9.9 Message Authentication Code
		ANSI X9.17 Financial Institution Key Management (Wholesale)
		ANSI X9.23 Message Confidentiality
		ANSI X9.30 Public Key Cryptography using Irreversible Algorithms
		ANSI X9.42 Symmetric Algorithm Keys using Diffie-Hellman.
		ANSI X9.45 Management Controls using Digital Signature & Attribute Certificates
		Network Public Key Encryption (RSA)

HHS Service Area	Candidate Standards
Network Security	NCSC-TG-005 (Network Interpretation) (C2 Implementation)
Database Security	NCSC-TG-021 (DBMS Interpretation) (C2 Implementation)